Organizational Power and Information Security Rule Compliance

Ella Kolkowska, Gurpreet Dhillon

Organizational power and information security rule compliance

Ella Kolkowska and Gurpreet Dhillon

Swedish Business School, Örebro University, Sweden
School of Business, Virginia Commonwealth University, USA

ella.kolkowska@oru.se, gdhillon@vcu.edu

Abstract. This paper analyzes power relationships and the resulting failure in complying with information security rules. We argue that inability to understand the intricate power relationships in the design and implementation of information security rules leads to a lack of compliance with the intended policy. We conduct the argument through an empirical, qualitative case study set in a Swedish Social Services organization. Our findings suggest a relationship between dimensions of power and information security rules and the impact there might be on compliance behavior. This also helps to improve configuration of security rules through proactive information security management.

Keywords: dimensions of power, information security, security compliance

1 Introduction

Lack of compliance with security policies occurs because of a number of reasons. Foremost amongst them are the inability of the policy to reflect current practices [1] and stakeholder resistance to security rules [2]. The organizational studies literature has intricately linked the concept of resistance to organizational power [3, 4]. Following on from the arguments presented in the dominant literature, we make a call to better understand organizational power in the context of information security policy compliance. Information security policy consists of a number of rules for protecting information in an organization. Whenever security rules are implemented or modified, there is a resultant organizational change - business processes get re-engineered, reporting structures get modified, technical controls get redesigned. However as Hardy [5] suggests, organizational power provides the energy to realize change. Thus, we argue that by developing a good understanding of organizational power dimensions it would be possible to ensure better security rule compliance. Correspondingly we also argue that a better appreciation for organizational power will ensure correct configuration of security rules.

The objective of the paper is to apply Hardy's dimensions of power to understand compliant and non-compliant behavior. Our findings also suggest how managers can use such an understanding to improve compliance with security rules. Three classes of definitions ensue from our argument - organizational power, information security and

compliance. In this paper we refer to organizational power as "the probability within a social relationship of being able to secure one's own ends even against opposition" [6]. We refer to information security as the protection of all information handling activities, may these be technical or non technical [7]. And compliance refers to a "relationship in which an actor behaves in accordance with a directive supported by another actor's power, and to the orientation of the subordinated actor to the power applied" [8 pg3].

2 Security Rule Compliance and Organizational Power

In a seminal paper Ranson et al [9] while discussing specialization of tasks in organizations, have argued that over time the path of internal differentiation leads to a "process of perpetual fission that fragments the collective enterprise of adequate understanding". This means that over time, in any enterprise, as complexity sets in, organization power is bound to get manifested. Hence compliance with a certain "paradigm or problematics" [cf. 9] is an attempt to articulate the latent relationships amongst stakeholders.

In the context of our research, and in using Ranson et al [9] terminology, a security rule is a form of organizational structure, which has its own "devotees". With time security rules get transformed (i.e structures evolve) as do the "devotees". The constant interplay between the evolving structures and those who believe in them results in *power*, which as Hardy [5] notes, helps in "bringing about strategic action". In the literature this interplay has been termed as structures being "constituted and constitutive" [see 9, 10].

Therefore in this section we explore the relationship between organizational power and security rule compliance. It is important to address this issue since dominant literature illustrates a rather consistent pattern of lack of compliance with security rules [11-14]. The notion of lack of compliance as a consequence of organizational power manifestations has been well documented in the literature. Lapke and Dhillon [2] identified resistance to security policies as one of the major reasons for failure. Lapke and Dhillon [15] also consider the importance of understanding organizational power in formulation and implementation of security policies. While aspects of compliance have been touched upon in the work of Lapke and Dhillon [2, 15], they do not explicitly focus on organizational power and it's utility (or limitation) in security rule compliance.

Another stream of security rule compliance research has focused on sanctions. The emphasis of this stream has been on studying the relationship of penalties and pressures that one party might apply on the other. Organizational power that comes into play in the context of penalties and sanctions is generally coercive in nature [16]. Coercive power and rewards have been extensively researched in the management literature. In the context of information security as well, a number of researchers have argued that coercion, sanctions and rewards have a significant impact on compliance or non compliance [17, 18]. This orientation has lead to using deterrence theory to suggest that individual expectations about external contingencies (e.g., rewards, punishments, etc.) are a driving force that directs their compliant behaviors [19, 20]. The emphasis within such behavioral research [17] is on the modification of one kind

of attributes (value congruence, legitimacy, etc) or another, to ensure compliance [see 21, 22, 23].

Some behavioral studies emphasize the importance of value correspondence and cultivation of a security culture. According to these studies compliance can be improved if employees internalize information security values in their daily work practices [24]. In this way "proper" security behavior will become a natural part of an employees' daily work activities [23, 25]. A similar approach is also suggested in 'awareness studies' [26]. These studies suggest that increased security awareness of employees and educational programs leads to better compliance with information security rules [27, 28].

There is no doubt that compliance with security rules can be achieved by any or all of the above identified approaches and clearly there may be more. However a limited number of current studies in the area emphasize the relationship between compliance behaviors and the sociological constructs such as power, which can be utilized to enforce these behaviors. Our study addresses this gap showing the value of applying the dimensions of power to understand compliant and non-compliant behaviors. This is because it allows for clarity on the nature and scope of exiting domination and how it plays out in the context of a strategic change, particularly when a new security rule gets instituted.

Organizational power and its implications on various aspects of business have been well researched and there are a number of conceptions of power. In recent years the work of Cynthia Hardy has had a profound impact on organizational [see 5] and information systems research [see 29]. From Hardy's [5] perspective, power is defined in neutral terms as a force that affects outcomes and allows beneficial results for all involved actors. She suggests a four dimensional framework that helps in understanding the consequences of organizational power from multiple perspectives. While other conceptions of power, particularly Clegg's [30] Circuits of Power have been widely used in information systems and security research, their discussion and comparison with Hardy's conceptualization goes beyond the scope of the current paper.

3 Theory and Methodology

In this section we present theory and methodology used in the conduct of our research.

3.1 Dimensions of Power

According to Hardy's [5] conceptualization of organizational power, it operates along four dimensions: resources, process, meanings and systems. While such an understanding of power has not been used in the information security literature, Dhillon [29] has articulated the dimensions to address IT implementation issues. The dimensions are discussed below.

Resource based power. Hardy contends that resource based power relates to the control that a given individual, group or a role might have on a range of resources

available in an organization. Such accumulation of power results in a "carrot" and "stick" situation, which translates to an ability to offer rewards, punish or impose sanctions. Proponents of resource-based power argue that leveraging such power can result in behavioral modification. Critics however argue that repeated use of resource-based power can be counter-productive.

Process based power. Business processes embody the values and norms of organizations. The power of processes challenges the notion that the decision process is open to participation by all interested parties in an organization. In fact, decision processes may be carefully designed to prevent those without power from gaining power by participating, thus protecting the status quo. Process based power can be changed by creating awareness and by opening up processes to new participants, issues and agendas. Such awareness helps sustain new behavior as long as it remains within existing values and norms.

Meaning based power. Power residing in meanings focuses on preventing conflict (i.e. resistance). Conversely, a lack of appreciation of meaning of action, causes resistance. Proper "indoctrination" of less powerful members in organizational customs and hierarchies leads to unquestioning acceptance of their role in the organization, thus preserving the status quo. Through the symbolic use of icons, rituals and language, change is given a new meaning, making it appear legitimate, desirable, rational or inevitable. Changes in some underlying values and norms may be possible. However changes in behavior are usually difficult.

System based power. Townley [31] succinctly describes system based power as "constituted through correlative elements of power and knowledge" p. 522. Power of a system is intertwined throughout all aspects of an enterprise. It cannot be mobilized without the other three dimensions: resources, processes and meanings. System based power is often taken for granted since it lies in the unconscious acceptance of "way things get done" in an organization. System based power is the backdrop against which decisions get taken.

In this paper we show the value of applying the dimensions of power to understand compliance and non-compliance and also to show how managers can mobilize those power dimensions to improve compliance with a security policy. Our contribution in relation to the earlier studies is thus the normative knowledge about how compliance can be improved by mobilizing suitable power dimensions. In the study we apply Hardy's [5] multidimensional framework of power. The framework was successfully used in earlier studies [29] related to IS implementations. We chose this framework for this study because of its value in realizing strategic changes in organizations. We argue that enforcement of security policy in an organization results in radical change i.e. enforcement of security policy is often met with resistance because it necessitates changes in business logic and existing business practices. Such situations are usually a consequence of a combination of resources certain stakeholders may have access to or a lack of clarity in the formal organizational procedures. As a result, meaning of stakeholder actions often remains ambiguous.

3.2 Research Methodology

The study was conducted via a qualitative case study [32, 33] at one of the Swedish Municipality Social Service Divisions responsible for helping vulnerable children and

their families. The case study was divided in two parts. The aim of the first part is to create an understanding about the organization and to identify relevant actor groups for studying power relationships. The second part focuses on finding power dimensions that were utilized to influence employee action, their awareness and values related to information security rules.

Data was collected in two phases. In phase one, interviews were conducted and project documents reviewed. Sixteen group interviews with eight different stakeholder groups (including management, system owners, IT-technicians and five user groups) were conducted. Each group included 5-6 people. The interviews focused on identifying and evaluating information flows as handled by the integrated computer based systems within the organization. In our initial analysis, two stakeholder groups emerged as central to use of power in security policy compliance. These were (a) managers who enforced the new security rules and processes through the information system and (b) care providers who did not comply with these rules.

In phase two, document analysis and in-depth interviews were conducted with two actor groups: managers and care providers. The emphasis was on finding different means of power that managers utilized to enforce new security processes and rules. Interviews with social services care providers were also conducted. These helped in interpreting what the respondents felt regarding their actions, awareness, values and perceptions with respect of security rules and processes. The respondents were chosen from all treatment centers. The number of respondents was not pre-determined. Once a saturation level was achieved, further interviews were not conducted. An interview guide helped in conducting the interviews, which mapped onto areas corresponding to information security rules within social services. This helped us in being comprehensive in our data collection efforts. Suitable probes were used and the data was correlated with informant insights. Each interview lasted approximately 1-2 hours. All interviews were tape recorded and transcribed. The data was also related to Hardy's [5] theory on dimensions of power. Particular attention was placed on identifying different means by which power was utilized. These were then classified as per the dimensions. The impact of power on actions, awareness and values was also interpreted.

4 Analyzing Power Dimensions and Information Security Compliance

In this section we analyze the case from a power perspective to understand how different dimensions of power were mobilized to drive the change of work practices in social services and how the changes resulted in compliant and non-compliant behaviors.

4.1 Case Background

In the information security policy at our case study organization, security was defined as: protection of information and information systems to achieve organizational requirements for availability, integrity, confidentiality and traceability. To meet the

requirements for information security the municipality board decided that all actor groups working in the municipality's social services were obligated to use an implemented IS for communication and exchange of information. According to the system owners, the information security rules and legal requirement were implemented in the system. Though all actor groups were obligated to comply with the decision taken by the municipality board, it was noticed that one actor group, the care providers at treatment centers, did not comply with the new rules. This lack of compliance caused information security problems related to confidentiality, availability, integrity and traceability. As a result managers were concerned about confidentiality of information and privacy of the clients. Other actor groups also could not access the up-to-date information and consequently their job performance suffered. Because of the problems the organization was also exposed to significant legal consequences, which could potentially have an impact on the viability of the enterprise.

4.2 Power of Resources

To improve information security, the municipality board decided that all actor groups within social services were obligated to use a computer-based information system for communication and exchange of information. The information system was implemented in all divisions of the social services. A special module supporting care provider work processes was included in the system. Significant time was allocated for training users. Resources were also allocated to IT-support teams. This ensured support of new users with respect to the system. Furthermore consultants who would be responsible for training of the users were hired.

After implementation of the computer-based information system, all documentation of social work at the treatment centers was supposed to be done in the system. However the care providers were confused about the processes, goals and requirements related to the new way of documenting. Before implementation of the system, paper-based documentation was mainly used as a means for communication between care providers working at a treatment centre. It was therefore clear as to *what* and *why* with respect to documentation. However following the implementation it was unclear as to what should be documented and to what extent. It was also unclear what the main goal with the documented information was. The system had also some serious deficiencies. For instance templates for some important documents were missing in the system and also the system did not support all work processes at treatment centers forcing users to use other resources such as word (for templates) and USB sticks for exchanging information.

In summary, resource based power utilized by managers partially influenced care providers behaviors related to documentation of social work. Care providers did begin documenting information using the implemented system. And they did find the system easy to use and were very satisfied with the technical support they got. However because of confusion regarding the new processes and the deficiencies in it the users developed their own routines relating to handling of information. Moreover there were no information security rules that regulated these routines. Consequently confidential information was exchanged with help of insecure portable devices and saved as Word files at local unprotected hard drivers. Same information could be

documented at different places (manually and digitally) at the same time with risk for loss of integrity. The information was also registered in the system too seldom and consequently not available for the other actor groups when they needed it.

4.3 Power of Processes

Using the information system to communicate and exchange of information meant changes in care provider work processes and responsibilities. Care providers were used to very detailed, papers-based notes to exchange information within a team and at treatment centers. All care providers were responsible for preparing these notes so that no information would be missing. They also had frequent contact with other actor groups. During these contacts it was possible to explain and clear up eventual misunderstandings, as well as to communicate the interpretive dimension of the work. According to care providers this dimension was very important in their work. At meetings with other stakeholders, care providers were responsible for presenting a rich picture of the situation, while care officers were responsible for choosing the relevant information and registering it in the system. In case of exceptional circumstances the responsible care officer was informed immediately by phone or e-mail and then the situation was discussed.

After the system was implemented the care providers were responsible for choosing the relevant information for other actor groups and for registration of that information in the information system. Awareness about the new processes for documentation was created by training and educational courses. The courses focused on functionality in the system and also explained that the registered information should be short and focus on facts. Although the new awareness was created during the courses, care providers still used the old way for communicating and exchanging educational information. The reason for that was conflict between the new processes and care provider work values. Documentation in the system was experienced as limiting because it required formal reporting (only facts), while their work was based on interpretation and observations. For the care providers, integrity and availability of information meant that information was detailed and included both facts and interpretations. These values were impossible to achieve according to the new rules because it was difficult to communicate the emotional and interpretive dimension through the system. In summary, the process-based power utilized by management did create awareness about new processes, however the awareness did not satisfactorily influence care providers behavior because it clashed with their own work values.

4.4 Power of Meaning

Power of meaning was not utilized by management in this case. The implemented information system was supposed to improve information security in the organization by enforcement of embedded information security rules. It was assumed that employees in social services were both aware of and aligned with existing information security rules. There was also a strong security culture amongst care providers at the studied treatment centers. In particular confidentiality and privacy

were emphasized as two core values. Care providers pointed out that security awareness was very important in their work. Even prior to the computerized systems, sensitive client information was handled very carefully - paper-based notes were locked in special rooms; the old paper-based notes were destroyed, etc. In spite of high information security awareness, care providers did not usually comply with the security rules, since the rules clashed with their own values related to integrity and availability of information.

4.5 Power of System

Power in the system is considered as the status quo and exists in "taken for granted" values, traditions, cultures and structures [5]. This dimension of power is often beyond the reach of organizational members. Hence to make a change, managers must utilize the other three dimensions of power: resources, processes and meanings.

In our case study organization, managers wanted to improve information security through the implementation of a computer-based information system. The managers relied mostly on power of resources in trying to change employee behavior. By creating a suitable environment and allocating resources for implementing the system and for training of the employees, managers did succeed to partially change employee behavior. However the ambiguity regarding the new processes and responsibilities created confusion amongst employees. Because of the unclear requirements for the new behavior, it was also impossible to fully deploy the power of resources to direct the behavior to support the new processes. While the power of resources did create some awareness about new processes and responsibilities, the training rendered was insufficient to change underlying values concerning communication and exchange of information. Thus the management failed to use power of meanings to change employee underlying values and norms so as to give the processes a new meaning. This resulted in the information security goals remaining under achieved.

5 Discussion

Four implications seem to emerge. These are based on our case study data. Space limitations however forbid us from going into sufficient details.

1. It is important to consider that an information security rule might involve strategic changes. As described in the case study section, the social services organization implemented most of the security rules as part of the computer based information systems. While some of the rules already existed in the organization, many new ones were also created. From a system administration perspective, implementing security rules simply amounted to careful design of rules into the computer-based systems and then implementing them in the organization. The ongoing argument in the organization was that if the integrated system were used for communication and exchange of information, it would ensure compliance with the security rules. As one of the administrators succinctly put it:

> Compliance with security rules is really a function of ensuring the **all** [emphasis added] organizational communications and information handling took place through the technical system.

This meant that the organization never saw the need to focus on establishing responsibility structures or establishing process descriptions, particularly when new rules were instituted. In the information security literature such perspectives have been termed as 'technically skewed' for a largely socio-technical problem [34]. In our case study organization, the implementation of the system largely occurred because of the power that resided with the administrators. Hence a combination of resource based and process based power was exerted. While the power ensured the implementation, the system forced differing interpretations of rules across the social services. One of the case-workers noted:

> It is practically impossible to use the system since it does not reflect the way we work. The checks and balances that have been built into the system are not necessarily the way in which any of the case-workers operate.

In dealing with such situations, Hardy [5] suggests that by managing meanings, resources and process, it is possible to "redefine the strategic initiative and the changes on which it hinges, as legitimate" (Pg. S10). This helps in creating awareness about the new structures and processes and hence making it possible to control behavior through the deployment of specific resources.

2. New security rules come embedded with structural changes, which require mobilization of power residing in the systems to ensure success. Implementation of a security rule constitutes significant structural changes. Since such changes are typically institutionalized in the organization, it requires a careful consideration of values, traditions and sub cultures. Failure to do so, results in systematic bypassing of the rules or circumventing controls. It occurs largely because of the "we don't do things in such a way here" attitude. In our case study organization, a social worker noted:

> We have been given the new system to undertake work in an efficient manner. I must say that it is not working. For, the new access rules mean that we have to wait for approvals through the chain of command. Unfortunately when one is with a client, they have to take decisions instantaneously. In such instances, we simply do not use the system. ....now I know that this can have possible security and compliance ramifications, but at the same time I have a job to do and services to render.

A typical approach of the management is to come in with a heavy hand, thus using either the power by virtue of the resources or their control of the processes. This however can be counterproductive. Hardy [5] suggests that instituting changes of this kind is a laborious task where work needs to be done in establishing proper buy-in. This ensures that there is a gradual shift in the prevalent ways of working.

3. New security rules have the potential to introduce value conflicts. Mobilizing power of meaning is important to avoid such conflicts. Whenever new security rules are implemented, they challenge the conventional interactions amongst organizational stakeholders. This usually has the potential for causing value conflicts. Value conflicts result in misinterpretation of meanings. From a dimension of power perspective, the power that resides in the meanings needs mobilization such that there is correct interpretation of the rules. In the literature, such misinterpretations have been linked to information security problems [see 35]. In our case study as well, the IT staff felt that there seemed to be a lack of common understanding as to how the work needs to be carried out. One IT staffer noted:

> I don't understand this. There are usually no complaints about the system. Everything works. However many people do not seem to use it. The new social workers who use the system seem to come up with interpretations are that are either different or in disagreement with the experience of the older social workers.

Various researchers stress that conflict and resistance is a natural consequence of applying power of resources and processes for realization of strategic change. Consequently managers who want to avoid employee resistance have to engage a power of meanings to legitimize their decisions. Lukes [36] has argued that power of meanings is often used to shape perceptions and cognition so that individuals do not question the status quo. The literature also terms this kind of power as "management of meaning" [37] where an individual may legitimize and de-legitimize so as to accept the viewpoint. Various symbols are typically used in this process - redundancy compensation, consultation, good will etc.

4. Power residing in resources, processes, meanings and systems needs to be mobilized to ensure awareness of values to achieve compliance with information security rules. In the studied case, the management failed to create an understanding of the new security processes and the new security rules. Moreover they did not succeed in changing underlying employee values that would affect change in employee behaviors. Consequently the new rules were not fully accepted and employees did not comply with these rules causing problems related to confidentiality, integrity and availability of information. In response to this problem, the organization got involved with a major awareness campaign, focusing on consequences of non-compliance. However the employees did not receive the awareness campaigns. This resulted in significant resistance among the user cadre. One user noted:

> They were bombarding us with all this awareness literature. They were also threatening us about the consequences of non-compliance. Nobody however focused on the reasons why people were not complying to the security rules.

The above observation by one user is a reflection of the state of affairs. In the literature, researchers have argued for awareness about the values rather than awareness about consequences of non-compliance [38]. Hardy [5] suggests that managers can redefine the strategic initiative by mobilizing power in a coordinated manner so as "to influence actions, awareness and values, and avoid both inertia and confusion" (Pg. S11)

6 Conclusion

In this paper we have evaluated power relationships in a social services organization and analyzed their impact on information security rule compliance. While majority of information security research has focused on overcoming resistance through sanctions, we take the position that a better understanding of power relationships helps overcoming resistance to information security rules and hence improve compliant behavior.

In our case study organization the management had failed to realize their plan to improve information security and had fallen short of improving the structures,

processes and values. Problems occurred because of two issues. First, the power residing in the organizational structures was not adequately understood. Second, power was only understood in terms of resources. This meant that majority of power exercise resulted in curbing access to resources. While resource based power may work in many cases, it has to be articulated in light of other kinds of power as well. In summary, the paper offers four key findings: 1) It is important to consider that an information security rule might involve strategic changes; 2) Strategic change requires mobilization of power of resources, processes and meanings and understanding of power embedded in the existing system; 3) Mobilizing power of meaning is important to avoid value conflicts; 4) All dimensions of power need to be mobilized to change actions, awareness and values. This will help in achieving compliance with information security rules.

7 References

1. Mattia, A., Dhillon, G.: Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. In: the IEEE Systems, Man & Cybernetics Conference October 5-8, Washington DC (2003)
2. Lapke, M., Dhillon, G.: A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study. In the Americas Conference on Information Systems (AMCIS 2006), Acapulco, Mexico (2006)
3. McFarland, D.A.: Resistance as a Social Drama: A Study of Change-Oriented Encounters. The American Journal of Sociology 109(6), 1249--1318 (2004)
4. Markus, M.L.: Power, politics and MIS implementation. Communications of the ACM 26(6), 430--444 (1983)
5. Hardy, C.: Understanding power: bringing about strategic change. British Journal of Management (7:Special issue), S3--S16 (1996)
6. Parson, T.: The structure of social action. Free Press, New York (1968)
7. Dhillon, G.: Principles of information systems security: text and cases. Wiley Inc., Hoboken, NJ (2007)
8. Etzioni, A.: A comparative analysis of complex organizations: On power, involvement, and their correlates. Free Press, New York (1975)
9. Ranson, S., Hinings, B., Royston, G.: The Structuring of Organizational Structures. Administrative Science Quarterly 25(1), 1--17 (1980)
10. Benson, J.K.: Organizations: A Dialectical View. Administrative Science Quarterly 22(1), 1--21 (1977)
11. PWC: Security Breaches Survey 2008. Enterprise and Regulatory Reform (BERR). PricewaterhouseCoopers on behalf of the UK Department of Business (2008)
12. Whitman, M.E., Mattord, H.: Principles of Information Security. 3rd ed. Course Technology, Boston (2008)
13. Nash, K.S. Greenwood, D.: The global state of information security. CIO Magazine. PriceWaterhouseCoopers (2008)
14. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Computers & Security 24(2), 124--133 (2005)
15. Lapke, M. Dhillon, G.: Power relationships in information systems security policy formulation and implementation. In the 16th Annual European Conference on Information Systems (ECIS 2008), Galway, Ireland (2008)

16.Kim, S.H., Lee, J.: A contingent analysis of the relationship between IS implementation strategies and IS success. Information Processing & Management 27(1), 111--128 (1991)
17.Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2), 154-165 (2009)
18.Kankanhalli, A., Teo, H.H., Tan, B.C., Wei, K.K.: An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23(2), 139--154 (2003)
19.Straub, D.: Effective IS security: an empirical study. Information System Research 1(2), 225--270 (1990)
20.Straub, D.W., Welke, R.J.: Coping with systems risks: security planning models for management decision making. MIS Quarterly 22(4), 441--469 (1998)
21.Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W.: If someone is watchning, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems 18, 151--164 (2009)
22.Phanila, S., Siponen, M., Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. In 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (2007)
23.Thomson, K.L., von Solms, R., Louw, L.: Cultivating an organizational information security culture. Computer Fraud and Security (10), 7--11 (2006)
24.Thomson, K.L.: Information Security Conscience: a precondition to an Information Security Culture. In 8th Annual Security Conference, Las Vegas, NV, USA April 15-16 (2009)
25.Vroom, C., von Solms, R.: Towards information security behavioural compliance. Computers & Security 23(3), 191--198 (2004)
26.Puhakainen, P.: A Design Theory for Information Security Awareness. University of Oulu: Oulu, Finland (2006)
27.Siponen, M.: A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security 8(1), 31--41 (2000)
28.Furnell, S.M., Gennatou, M., Dowland, P.S.: A prototype tool for information security awareness and training. Logistics Information Management 15(5), 352--357 (2002)
29.Dhillon, G.: Dimensions of power and IS implementation. Information & Management 41, 635--644 (2004)
30.Clegg, S.: Frameworks of power. Sage Publications, London (1989)
31.Townley, B.: Foucault, power/knowledge and its relevance for Human Resource Management. Academy of Management Review 18(3), 518--545 (1993)
32.Benbasat, I., Goldstein, D.K., Mead, M.: The case research strategy in studies of information systems. MIS Quarterly 11(3), 369--388 (1987)
33.Myers, M.D.: Qualitative research in business & management. Sage Publications, London, UK (2009)
34.Hedström, K., Dhillon, G., Karlsson, F.: Using Actor Network Theory to Understand Information Security Management. In the 25th Annual IFIP TC 11, 20-23 September Brisbane, Australia (2010)
35.Dhillon, G.: Managing Information System Security. Macmillan, London (1997)
36.Lukes, S.: Power: a radical view. Macmillan, London (1974)
37.Pettigrew, A.M.: On studying organizational cultures. Administrative Science Quarterly 24, 570--581 (1979)
38.von Solms, R., von Solms, B.: From policies to culture. Computers & Security 23(4), 275--279 (2004)